

What is claimed is:

1. A method comprising:
 configuring a transmitter and a receiver to encrypt and decrypt, respectively, a data frame based on information included in a header of the data frame.
2. The method of claim 1, further comprising authenticating the header of the data frame.
3. The method of claim 1, further comprising:
 processing the header of the data frame to provide a processed header; and
 configuring the transmitter and the receiver based on information included in the processed header.
4. The method of claim 1 wherein configuring comprises:
 configuring the receiver to authenticate and decrypt a data portion and a message integrity code portion of the data frame.
5. The method of claim 4 comprising:
 decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message integrity code portion, respectively;
 calculating the message integrity code of the data frame from the decrypted data portion; and
 comparing the calculated message integrity code to the decrypted message integrity code portion.
6. The method of claim 1, wherein configuring comprises:

configuring the transmitter to authenticate and to encrypt the data portion and a message integrity code based on information included in the header of said data frame.

7. The method of claim 6, further comprising:
 - dividing the data portion into two or more blocks of a predetermined block size; and
 - padding a last block of the data portion with one or more zeros to match the predetermined block size.
8. the method of claim 1 further comprising:
 - generating an encryption vector to be used to encrypt and decrypt the data frame.
9. The method of claim 1, further comprising:
 - generating an authentication vector to be used to authenticate the data frame.
10. The method of claim 8, further comprising:
 - decrypting one or more encrypted portions of the data frame by performing an exclusive OR operation between the one or more encrypted portions of the data frame and the encryption vector.
11. The method of claim 8, further comprising:
 - encrypting one or more portions of the data frame by applying an exclusive OR operation between the one or more portions of the data frame and the encryption vector.

12. An apparatus comprising:
 - a transmitter to encrypt a data frame;
 - a receiver to decrypt the data frame; and
 - a configuration unit to configure the transmitter and the receiver based on information included in the data frame.
13. The apparatus of claim 12, comprising:
 - a security unit to provide an encryption vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.
14. The apparatus of claim 12, comprising:
 - a security unit to provide an authentication vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.
15. The apparatus of claim 13, wherein the receiver includes a decryption unit to provide a decrypted data frame by applying the encryption vector to an encrypted data frame.
16. The apparatus of claim 13, wherein the transmitter includes an encryption unit to receive an authenticated data frame and the encryption vector to provide an encrypted data frame.
17. The apparatus of claim 13, wherein the security unit comprises:
 - an advance encryption standard engine to generate the encryption vector and an authentication vector.
18. The apparatus of claim 13, wherein the security unit comprises:

a message integrity code generator to generate a message integrity code of the encrypted data frame and to calculate a message integrity code of a decrypted data message.

19. The apparatus of claim 18, wherein the security unit comprises.

a comparator to compare between the calculated message integrity code and a decrypted message integrity code.

20. An apparatus comprising:

a transmitter to encrypt a data frame;

a receiver to decrypt the data frame; and

a configuration unit to configure the transmitter and the receiver based on information included in the data frame.

21. The apparatus of claim 20, comprising:

a security unit to provide an encryption vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

22. The apparatus of claim 20, comprising:

a security unit to provide an authentication vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.

23. The apparatus of claim 21, wherein the receiver includes a decryption unit to provide a decrypted data frame by applying the encryption vector to an encrypted data frame.

24. The apparatus of claim 21, wherein the transmitter includes an encryption unit to receive an authenticated data frame and the encryption vector to provide an encrypted data frame.

25. The apparatus of claim 21, wherein the security unit comprises:
 - an advance encryption standard engine to generate the encryption vector and an authentication vector.
26. A wireless communication system comprising:
 - two or more stations wherein at least one station of the two or more stations includes:
 - a transmitter to encrypt a data frame;
 - a receiver to decrypt the data frame; and
 - a configuration unit to configure the transmitter and the receiver based on information included in the data frame.
27. The apparatus of claim 26, comprising:
 - a security unit to provide an encryption vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.
28. The apparatus of claim 26, comprising:
 - a security unit to provide an authentication vector to the transmitter and to the receiver based on the configuration of the transmitter and the receiver.
29. The apparatus of claim 27, wherein the receiver comprises a decryption unit to provide a decrypted data frame by applying the encryption vector to an encrypted data frame.
30. The apparatus of claim 27, wherein the transmitter comprises an encryption unit to receive an authenticated data frame and the encryption vector to provide an encrypted data frame.

31. The apparatus of claim 27, wherein the security unit comprises:
 - an advance encryption standard engine to generate the encryption vector and an authentication vector.
32. An article comprising: a storage medium, having stored thereon instructions, that when executed, result in:
 - configuring a transmitter and a receiver to encrypt and decrypt, respectively, a data frame based on information included in a header of the data frame.
33. The article of claim 32, wherein the instructions when executed, result in:
 - configuring the receiver to authenticate and decrypt data portion and a message integrity code portion of the data frame.
34. The article of claim 32, wherein the instruction when executed, result in:
 - generating an encryption vector to be used to encrypt and decrypt the data frame based on information included in a header of the data frame.
35. The article of claim 32, wherein the instruction when executed, result in:
 - generating an authentication vector to be used to authenticate the data frame.
36. The article of claim 32, wherein the instruction when executed, result in:
 - decrypting one or more encrypted portions of the data frame by performing an exclusive OR operation between the one or more encrypted portions of the data frame and the encryption vector.